

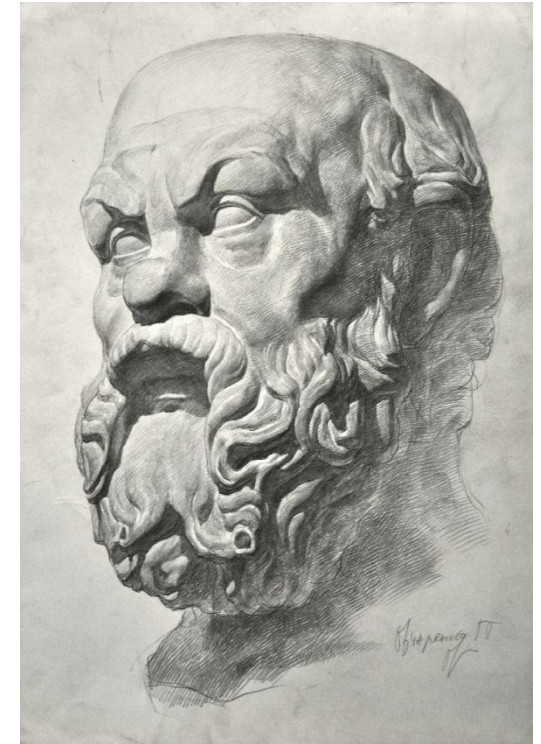


Комплексное противодействие атакам на
информационные и материальные
ресурсы бизнеса

Тема № 2

Защита персональных данных и иной конфиденциальной информации

Лекция, 2 часа

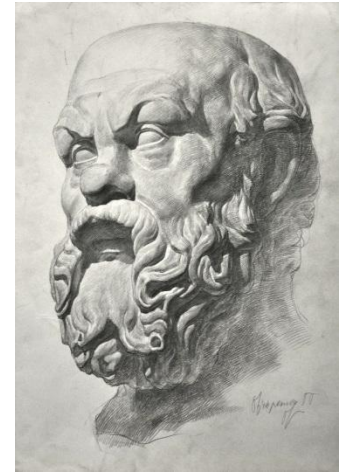


Сократ, мудрец

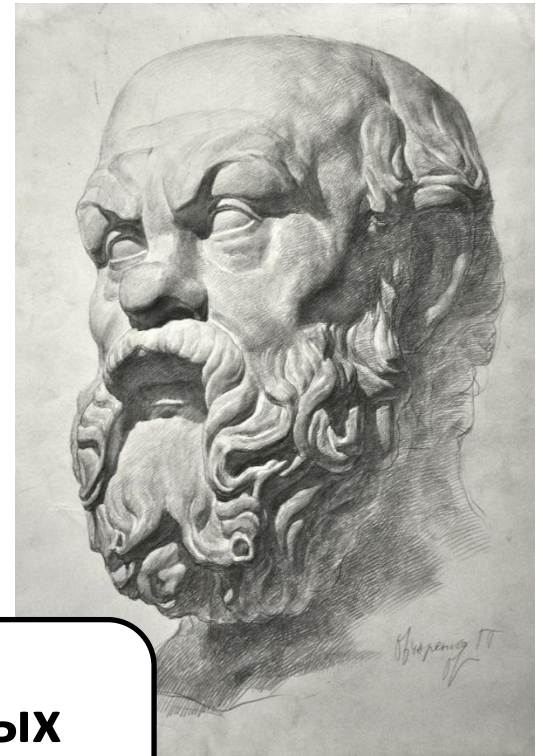
Информационная безопасность

Оглавление

1. Право личности на защиту персональных данных
2. Система защиты персональных данных в Российской Федерации
3. Защита персональных данных на предприятии
4. Ответственность за нарушение правил защиты персональных данных
5. Библиография



Право личности на защиту персональных данных



Сократ, мудрец

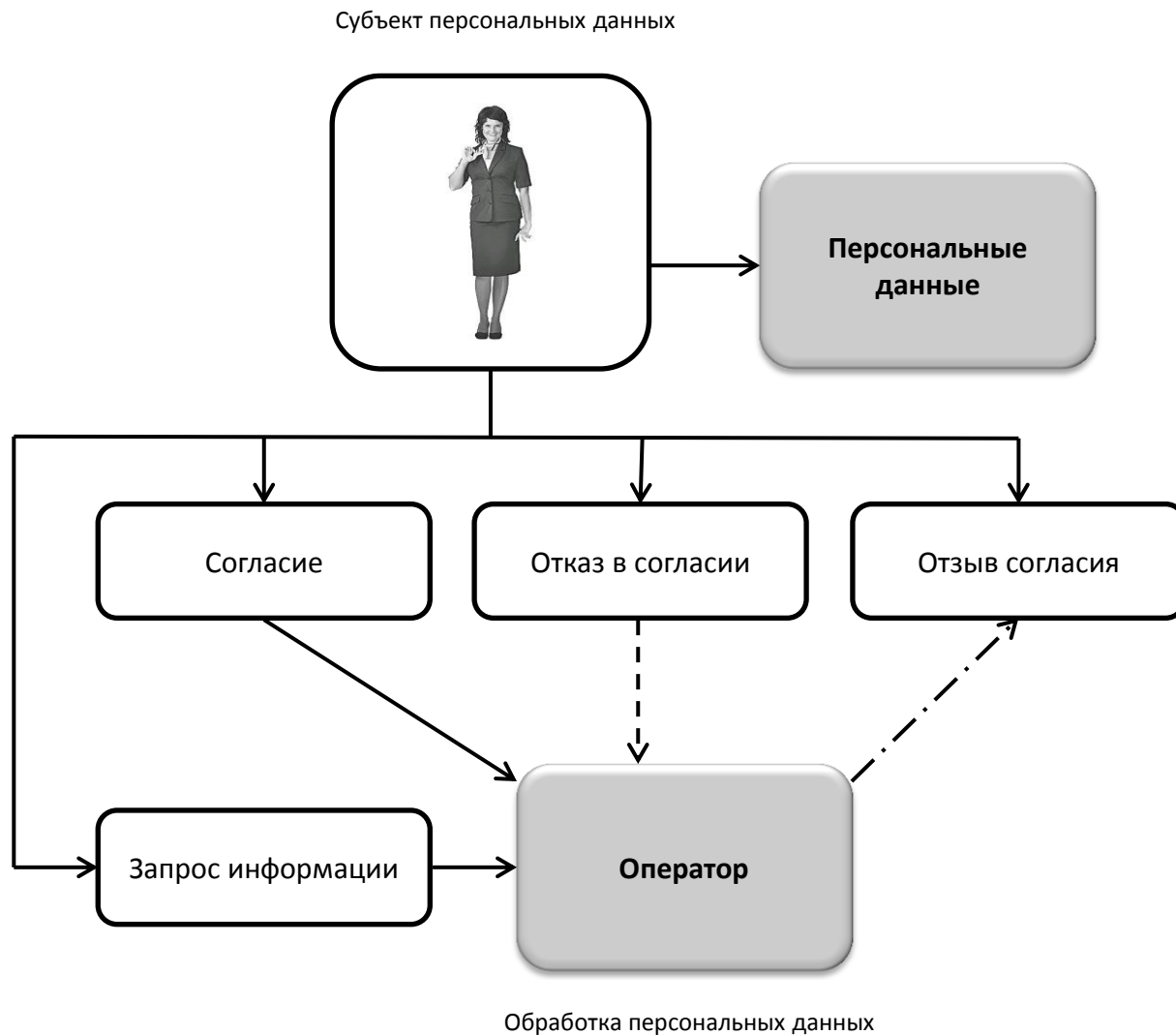
ЗАКОНОДАТЕЛЬСТВО ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ



ОПЕРАТОРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ



ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ





СУБЪЕКТ ВПРАВЕ ЗАПРОСИТЬ У ОПЕРАТОРА:

- 1) Подтверждение факта обработки персональных данных оператором;
- 2) Правовые основания и цели обработки персональных данных;
- 3) Цели и применяемые оператором способы обработки персональных данных;
- 3) Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 4) Обработываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- 5) Сроки обработки персональных данных, в том числе сроки их хранения;
- 6) Порядок осуществления субъектом персональных данных прав, предусмотренных настоящим федеральным законом;
- 7) Информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 8) Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 9) Иные сведения, предусмотренные настоящим федеральным законом или другими федеральными законами.

КТО ЗАЩИЩАЕТ ПРАВА СУБЪЕКТОВ ПДН?

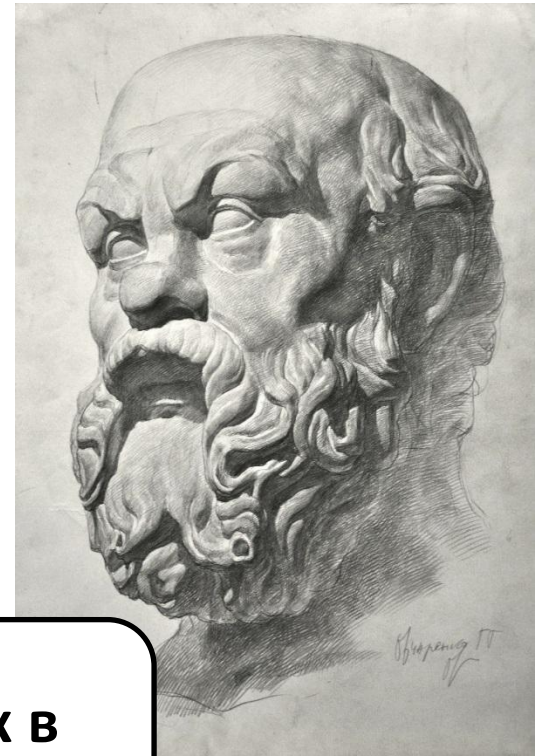
МНЕНИЕ ПРОФЕССИОНАЛОВ



Уполномоченным органом по защите прав субъектов персональных данных в настоящее время является **Федеральная служба технического и экспортного надзора Российской Федерации (Роскомнадзор)**. Она наделена широкими полномочиями и имеет право:

- ☐ Запрашивать и безвозмездно получать требуемую информацию у юридических и физических лиц;
- ☐ Осуществлять проверки собственными силами или с привлечением других органов;
- ☐ Требовать от оператора выполнения предусмотренных законом действий;
- ☐ Принимать меры по приостановлению или прекращению обработки персональных данных;
- ☐ Обращаться в суд с исковыми заявлениями в защиту прав неопределенного числа лиц;
- ☐ Направлять заявление в регулирующий орган оператора о приостановлении или отзыве лицензии;
- ☐ Направлять в правоохранительные органы материалы для возбуждения уголовных дел;
- ☐ Вносить предложения в Правительство Российской Федерации;
- ☐ Привлекать виновных лиц к административной ответственности.

Система защиты персональных данных в Российской Федерации



Сократ, мудрец

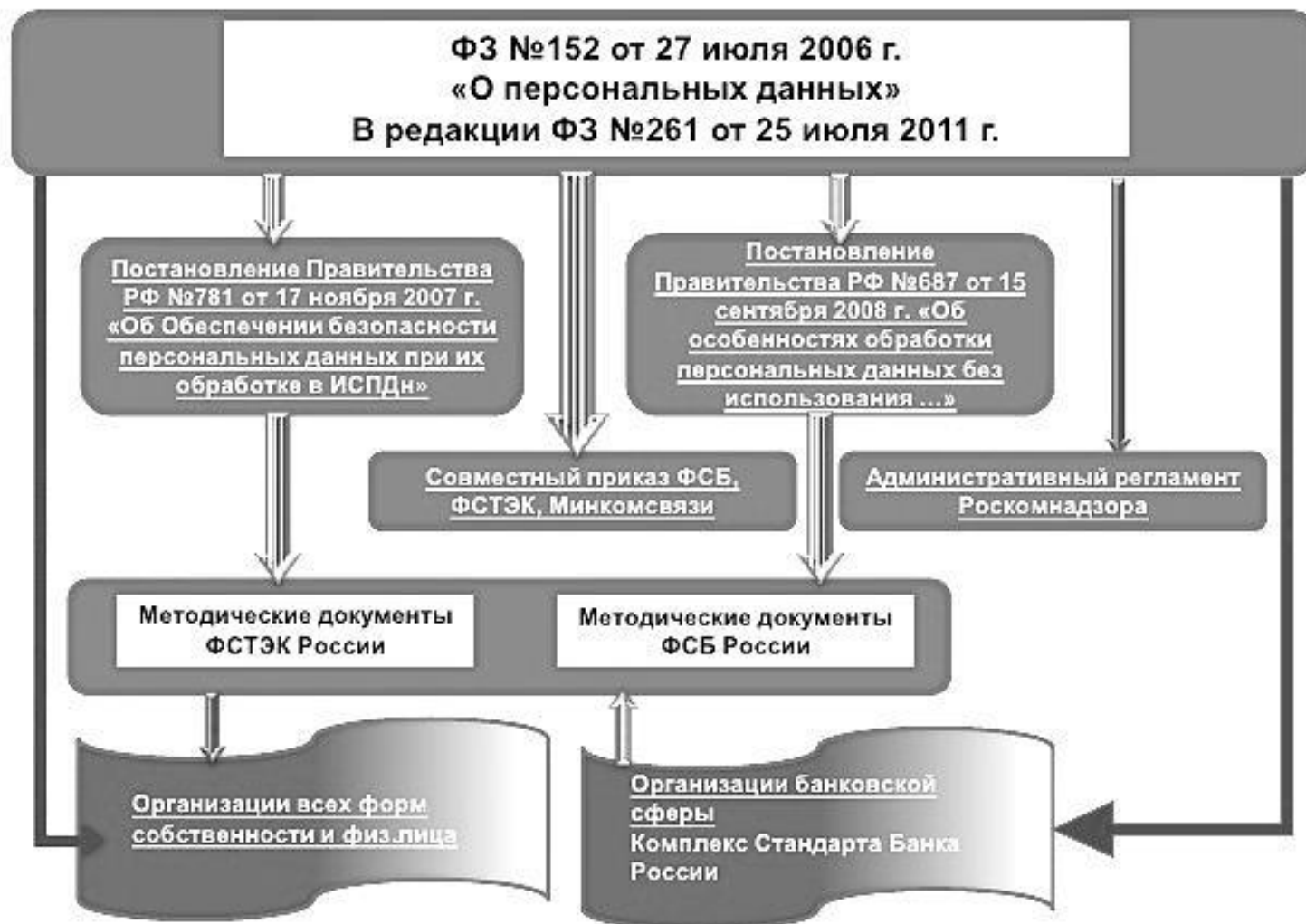
**ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 27 ИЮЛЯ 2006 ГОДА
№ 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»**



Статья 3. Основные понятия

- 1) Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2) Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- 3) Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- 4) Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;
- 5) Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)...

РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СЕГОДНЯ



ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ



Примечание: выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых оператором угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы...

(п. 1.4 Приказа ФСТЭК №58)

ОБЯЗАННОСТИ ОПЕРАТОРА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Правовые

- Обоснование законности обработки ПДн
- Уведомление уполномоченного органа до начала обработки ПДн
- Поручение оператора
- И др.

Организационные

- Назначение ответственного за организацию обработки ПДн
- Издание документов, определяющих политику Оператора
- Оценка вреда, который может быть причинен субъекту
- И др.

Технические

- Определение угроз безопасности
- Применение СЗИ, прошедших в установленном порядке процедуру оценки соответствия
- Обнаружение фактов несанкционированного доступа
- И др.

ОБЯЗАННОСТИ ОПЕРАТОРА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка ПДн

Неточные ПДн

*Неправомерная
обработка ПДн*

Блокирование ПДн

Подтверждение

Уточнить в
течение 7
рабочих дней

Прекратить в течение
3 рабочих дней. В
противном случае –
уничтожить в течение
10 рабочих дней

Обработка ПДн

*Достижение цели
обработки*

*Отзыв согласия
субъекта*

Прекратить обработку и уничтожить
ПДн в течение 30 рабочих дней

*Отсутствие возможности
уничтожения*

Блокирование ПДн и их
уничтожение в срок, не более 6
месяцев

КТО ТАКИЕ РЕГУЛЯТОРЫ?



ДЕЯТЕЛЬНОСТЬ РЕГУЛЯТОРОВ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

РОСКОМНАДЗОР

Уполномоченный орган по защите прав субъектов персональных данных:

- ✓ Государственный контроль и надзор за обработкой ПДн
- ✓ Ведение реестра операторов
- ✓ Применение мер профилактического и пресекающего характера, направленных на недопущение нарушений в сфере защиты ПДн

ФСТЭК России

Уполномоченный орган в области противодействия техническим разведкам и технической защиты информации

ФСБ России

Уполномоченный орган в области обеспечения криптографической и инженерно-технической защиты информации

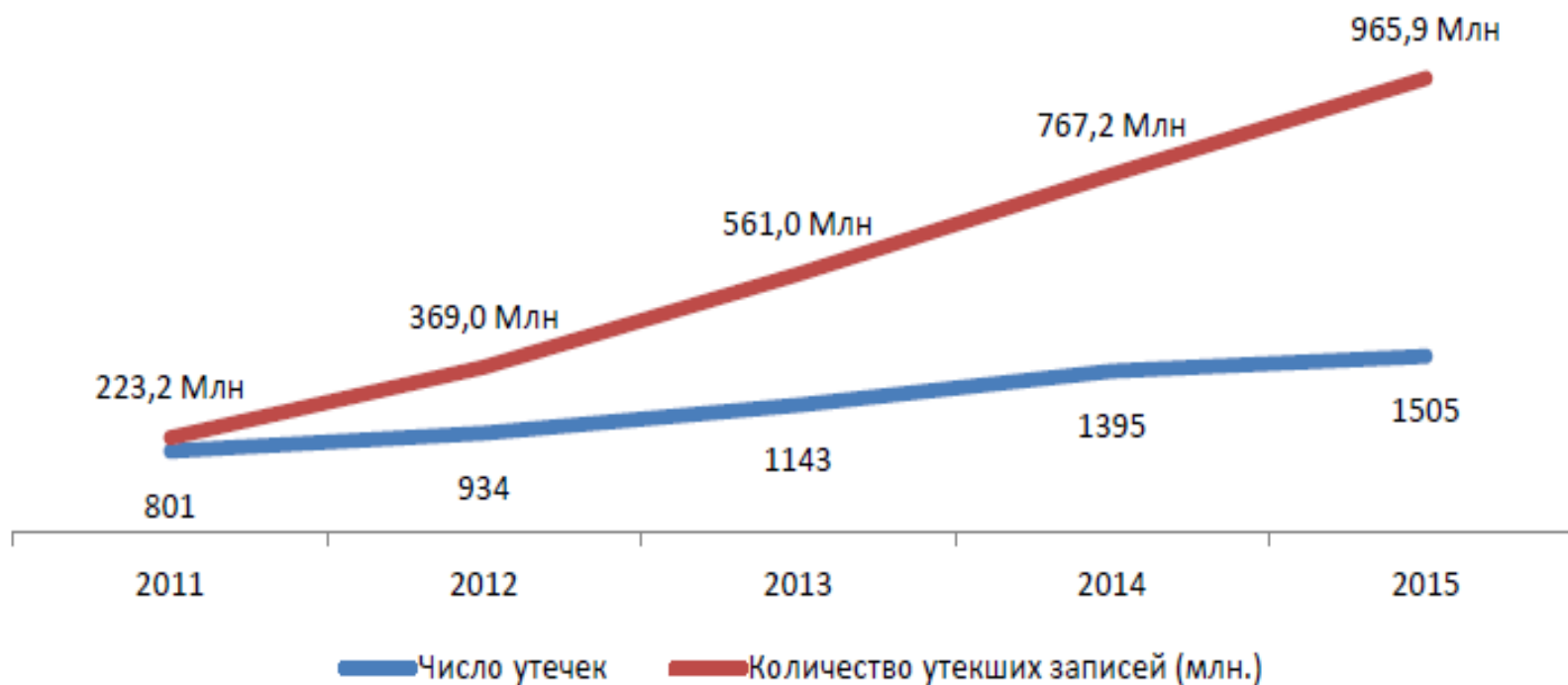
ФСТЭК России и ФСБ России определены как регуляторы для государственных ИС, однако, по решению Правительства, ФСТЭК России и ФСБ России могут быть регуляторами для определенных видов деятельности (не являющимися государственными ИС) без права ознакомления с ПДн

ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПРОВЕРОК РОСКОМНАДЗОРОМ



Срок проведения проверки – до 20 рабочих дней. При необходимости может быть продлен на срок до 20 рабочих дней.

СЛУЧАИ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПДН

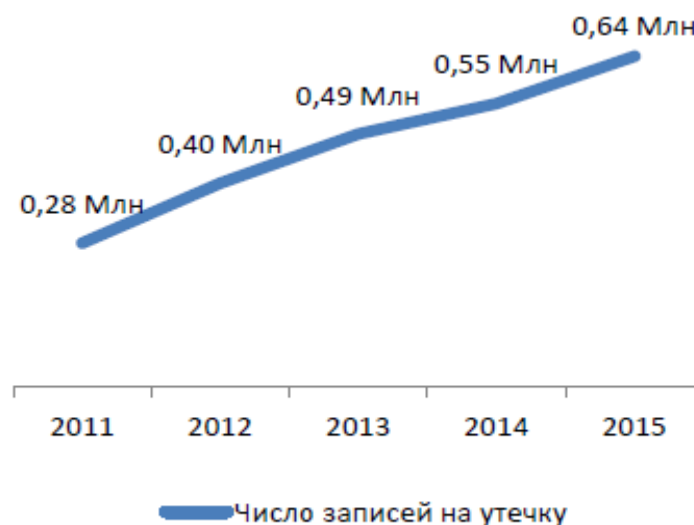


Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2011 - 2015 гг.

СЛУЧАИ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПДн

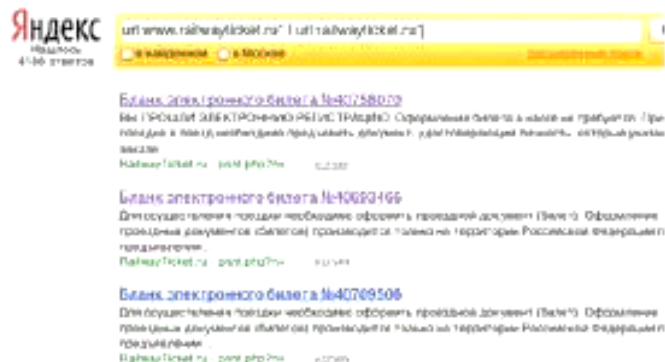


**Динамика роста числа утечек,
объема записей ПДн в 2011 -2015 гг.**



**Объем персональных данных,
скомпрометированных в ходе одной
утечки в 2011 -2015 гг.**

СЛУЧАИ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПДН



❑ успешный несанкционированный доступ к данным Интернет-сервисов PlayStation Network и Qriocity (77 миллионов учётных записей, апрель 2011)

❑ Номер телефона и текст СМС-сообщения Мегафон, МТС, Билайн (лето 2011)

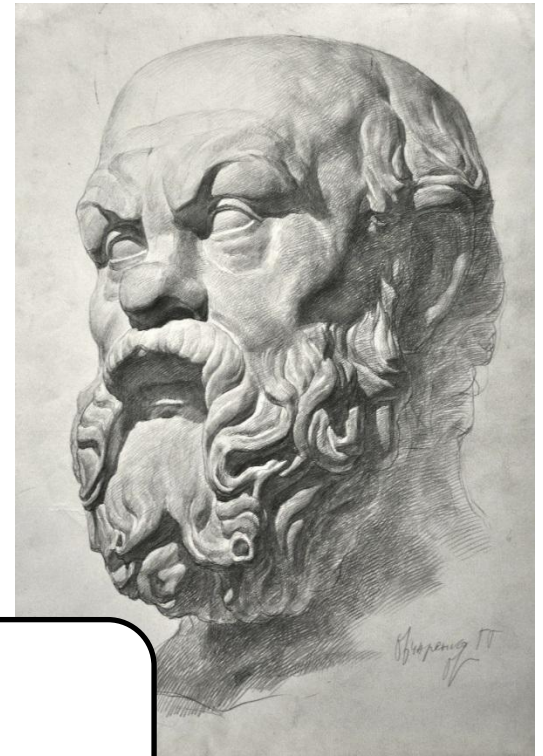
❑ ссылки на страницы со статусами заказов в различных интернет-магазинах (лето 2011)

❑ Электронные железнодорожные билеты с датами, номерами рейсов, именами пассажиров (лето 2011)

❑ Имена, фамилии, адреса и телефоны почти 1,6 млн абонентов МТС в Башкирии и Петербурге на сайте zhiltsy.net (осень 2011)

❑ и т.д.

Защита персональных данных на предприятии

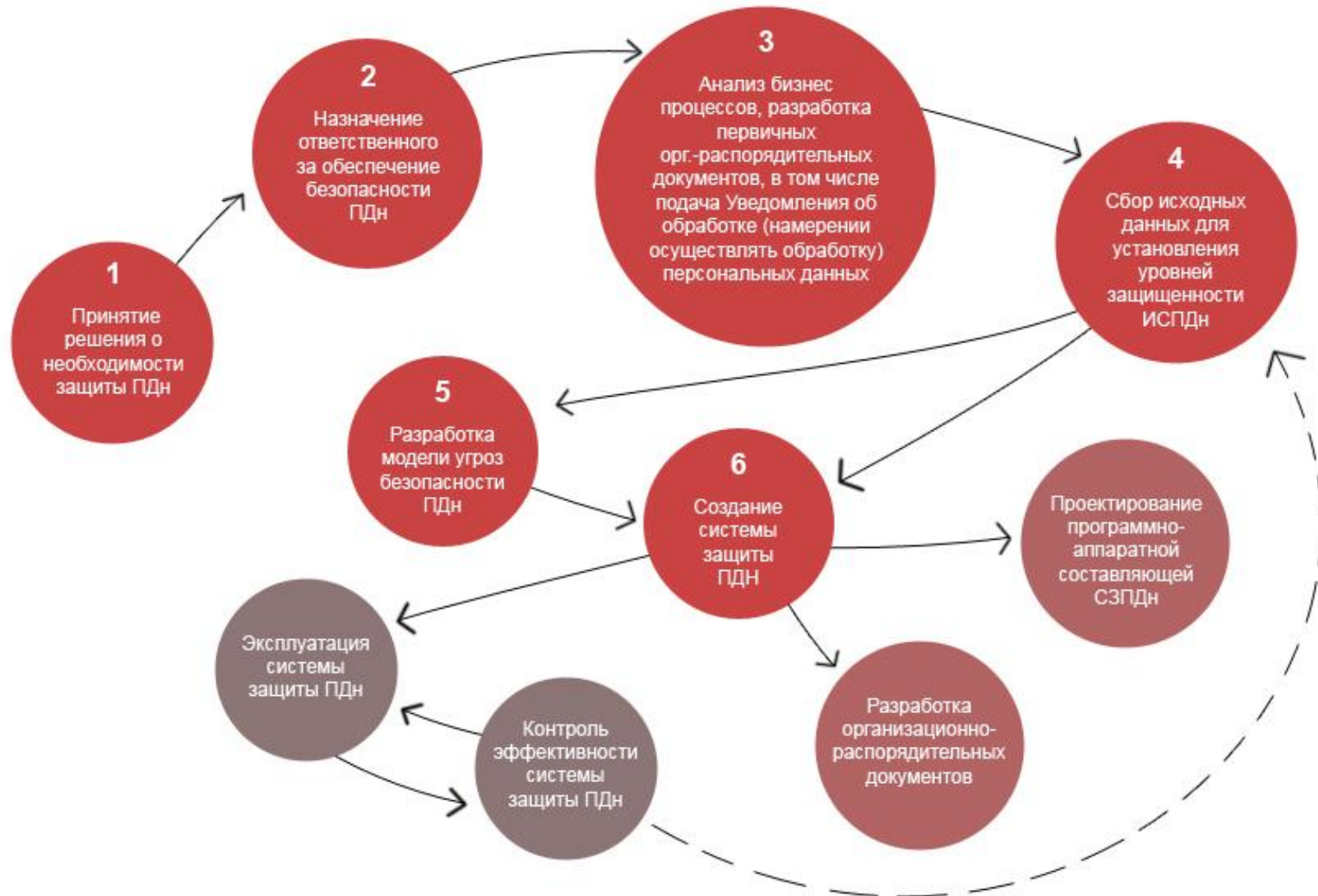


Сократ, мудрец

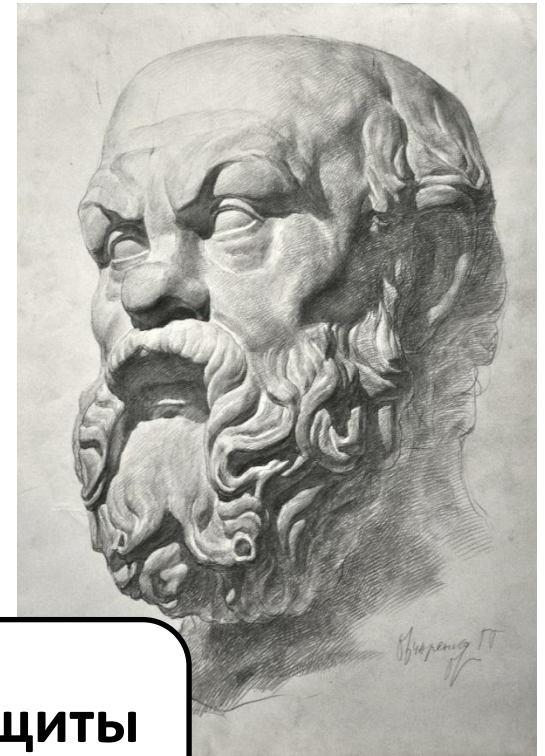
ЗАЧЕМ НАДО ТРАТИТЬ СИЛЫ И СРЕДСТВА НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ?



ЭТАПЫ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ



Ответственность за нарушение правил защиты персональных данных на предприятии



Сократ, мудрец

РИСКИ НЕИСПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА

Неисполнение требований 152-ФЗ влечет для бизнеса компании риски следующего характера:

- Гражданские иски со стороны клиентов или работников
- Приостановление или прекращение обработки персональных данных в компании
- Привлечение компании и (или) ее руководства к административной, уголовной, гражданской, дисциплинарной и иным видам ответственности
- Приостановление действия или аннулирование лицензий на основной вид деятельности компании
- Репутационные риски
- Риски недобросовестной конкуренции (приостановления деятельности компании с подачи конкурентов при имеющихся нарушениях правил защиты персональных данных)

ОТВЕТСТВЕННОСТЬ

ст. 24, 152-ФЗ: Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность

➤ **Дисциплинарная**

ТК РФ: статьи 81, 90, 195, 237, 391

Максимум: возмещение морального вреда сотруднику, получившему ущерб от разглашения его ПДн

➤ **Административная**

КоАП РФ: статьи 13.11, 13.12, 13.13, 13.14, 19.4, 19.5, 19.7, 19.20

Максимум: 250 000 р. + приостановление деятельности на срок до 90 суток + дисквалификация должностного лица на срок до 3-х лет + конфискация средств защиты

➤ **Уголовная**

УК РФ: статьи 137, 140, 272, 273, 274

Максимум: 300 000 р. + принудительные работы на срок до 4-х лет + арест до 6-ти месяцев + лишение права занимать должность на срок до 5-ти лет

ОТВЕТСТВЕННОСТЬ

Статья	Нормативно-правовой акт	Нарушение	Максимальная мера наказания
137	УК	Нарушение неприкосновенности частной жизни	Штраф до 300.000 руб. или в размере заработной платы или иного дохода осужденного за период до 2 лет, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательные работы на срок до 180 часов, либо исправительные работы на срок до 1 года, либо арест на срок до 4 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет
140	УК	Отказ в предоставлении гражданину информации о его ПДн, обрабатываемых организацией	200.000 руб., либо в размере заработной платы или иного дохода осужденного за период до 18-ти месяцев, либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет
19.5	КоАП	Невыполнение в срок требований надзорного органа или ФСТЭК РФ (при 3-х лет повторной проверке)	500.000 руб. + дисквалификация должностного лица до 3-х лет
13.11	КоАП	Нарушение порядка сбора, хранения, использования, распространения ПДн	и 10.000 руб.
19.7	КоАП	Непредставление или представление в не полном или искаженном виде сведений об операторе ПДн	5.000 руб.

ОТВЕТСТВЕННОСТЬ

Статья	Нормативно-правовой акт	Нарушение	Максимальная мера наказания
13.11	КоАП	Нарушение порядка сбора, хранения, использования и 10.000 руб. распространения ПДн	
19.7	КоАП	Непредставление или представление в не полном или искаженном виде в 5.000 руб. Роскомнадзор сведений об операторе ПДн	
13.12	КоАП	Нарушение правил защиты информации	20.000 руб. + конфискация + приостановление деятельности на срок до 90 суток
13.13	КоАП	Деятельность в области защиты ПДн без лицензии ФСТЭК РФ / ФСБ РФ	20.000 руб. + конфискация

Кейс

ЗАЩИТА ПДН В СУДЕБНОЙ ПРАКТИКЕ

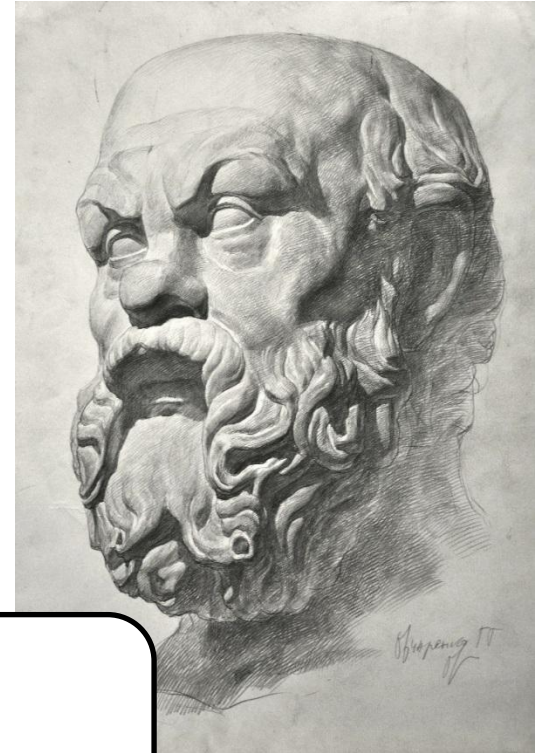


В 2012 г. Ярославский областной суд вынес апелляционное определение по жалобам коммерческого банка «Юниаструм Банк» и коллекторского агентства «Морган энд Страут» на решение Фрунзенского районного суда г. Ярославля. Суд первой инстанции признал незаконным действия банка по передаче персональных данных гражданина «Григорьева» коллекторскому агентству «Морган энд Стаут», обязал коллектора уничтожить персональные данные истца, взыскал с банка и коллектора денежные средства в целях возмещения морального ущерба, нанесенного гражданину «Григорьеву». В апелляционной жалобе «Юниаструм банк» поставил вопрос об отмене решения районного суда и направлении дела на новое рассмотрение.

Ярославский областной суд, рассмотрев апелляционные жалобы банка и коллекторского агентства на решение Фрунзенского районного суда г. Ярославля, в удовлетворении жалобы отказал. Областной суд исходил из того, что банк предоставил «Григорьеву» потребительский кредит на основании соответствующего договора. В связи с тем, что клиент перестал регулярно выполнять свои обязательства по кредитному договору, банк передал его персональные данные в коллекторское агентство для организации взыскания задолженности. При этом **в кредитном договоре не было прописано условие о передаче персональных данных заемщика третьему лицу в случае ненадлежащего исполнения им своих обязанностей по данному договору.** Банк также не запросил согласие «Григорьева» на передачу его персональных данных, а осуществил передачу самостоятельно. При этом судом также установлено, что передача прав требования от банка «Морган энд Страут» не было оформлено в порядке, предусмотренном законодательством. Ярославский областной суд. Апелляционное определение от 05.03.2012 г. по делу № 33-939/2012. Информационный ресурс [www/consultant.ru](http://www.consultant.ru) (дата обращения 02.02.2015).

Вопрос: каким образом, по вашему мнению, банк мог избежать нарушения законодательства.

Библиография



Сократ, мудрец

Основная литература

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. М.: Издательство «Юрайт», 2016;
2. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Пособие для обучения на майноре. (на начальном этапе)

Дополнительная литература

1. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Защита персональных данных в организациях. М.: Флинта, 2011;
2. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г.;
3. Агапов А. Б. Основы государственного управления в сфере информатизации в Российской Федерации. М.: Юристъ, 2012;

Нормативные акты

ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных».